IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Scott MOSKOWITZ	)	Group Art Unit: 2132
	)	
Application Number: 08/999,766	)	Examiner: D. Meislahn
	)	
Filed: July 23, 1997	)	
	)	
Title: STEGANOGRAPHIC METHOD	)	
AND DEVICE		

RECEIVED

OCT 3 0 2001

Technology Center 2100

BOX FEE AMENDMENT
Commissioner for Patents
Washington, D.C. 200231

Sir:

RESPONSE AND REQUEST FOR RECONSIDERATION
AFTER NOTICE OF APPEAL

On March 27, 2001, a "final office action" issued in this case. On September 27, 2001, Applicant filed a Request for a Three-Month Extension of Time and a Notice of Appeal, with the appropriate fees attached. Accordingly, Applicant believes that no further fees are required to submit this Response and Request for Reconsideration. In the event that fees are due, please charge such fees to the undersigned's Deposit Account No. 50-1129.

Applicant is requesting the Examiner to withdraw the finality of the last office action, and to withdraw the rejections of all pending claims for at least the reasons outlined below. Applicant submits that the pending claims are patentable and earnestly seeks a notice of allowance.

RESPONSE

I. FINALITY

The Examiner acknowledges that new grounds of rejection have been raised in the Office Action of March 27, 2000. Nonetheless, the Examiner asserts that the new grounds of rejection were necessitated by Applicant's amendment, and therefore made the action final.

1

Applicant requests the Examiner to withdraw the finality of the March 27 Office Action because the Examiner's "new rejection" is not necessitated by Applicant's amendment. In an interview with the Examiner and his Supervisory Examiner on December 13, 2000, Applicant urged the Examiner to withdraw the previous 102 rejections because those portions of Schneier being relied upon by the Examiner related to encryption—not steganography. At that time, the claims were directed, in part, to the use of a random key to steganographically encode independent information into a carrier signal. An agreement was reached, based upon constructive suggestions of the Supervisory Examiner, to amend the claim to recite a "steganographic key." Applicant agreed in substance because a key that encodes data steganographically is properly characterized as a steganographic key. (Applicant's actual amendment was to the use of a "stega-cipher" as disclosed in the specification). A conclusion was reached at the end of the interview as stated by the Examiner in the Interview Summary: "Language to overcome the rejection of claims 25 and 29 was agreed upon."

Because the claim (before amendment) was already directed to a key to steganographically encode independent data into the carrier signal, it is illogical to conclude that the amendment to recite a "stega-cipher" necessitated Examiner's allegedly new rejection. As stated in the MPEP :

> A second or any subsequent action on the merits in any application or patent involved in reexamination proceedings should not be made final if it includes a rejection, on prior art not of record, of any claim amended to include limitations which should reasonably have been expected to be claimed. See MPEP Section 904 et seq. For example, one would reasonably expect that a rejection under 35 U.S.C. 112 for the reason of incompleteness would be replied to by an amendment supplying the omitted element.

MPEP 706.07(a) (emphasis added). In view of the title of the application (namely, "Steganographic Method and Device"), and in view of the claim language prior to amendment ("using a random or pseudo random key to steganographically encode independent information"), the Examiner should have reasonably expected an amendment directed to a "steganographic key" as suggested by the Supervisory Examiner, or to a "stega-cipher" as recited

in the specification and as amended by Applicant. For at least this reason, the finality is premature.

Moreover, if the Examiner was relying on the new reference because of the amendment, then the new references should disclose a "stega-cipher" as claimed. This is clearly not the case. As discussed below, Examiner relies upon the new reference not because it discloses a "stega-cyper" key, but because it allegedly references "a pseudo-random key." **The use of this pre-amendment language makes clear that the Examiner is not relying on the new references to reject the newly added language.** Accordingly, the amendment did not necessitate the reliance upon the new reference, and thus, the finality of the rejection is premature.

II.   102 REJECTIONS

a)   Rejections Generally

The Examiner asserts that claims 25, 27-29, 31-33, 35, 62, and 63 are anticipated by an article entitled Techniques for Data Hiding ("Bender"). In particular, the Examiner asserts that a spread spectrum technique anticipates these claims: "In section 3.4, which studies spread spectrum environments, a pseudo-random key used to hide information is disclosed. The key, a carrier wave, and data are all combined." (Office Action at 2). Applicant disagrees that the cited section anticipates the claims.

In order for a reference to anticipate a claim, the reference must disclose each and every element of the claimed invention. Independent claim 25 recites, inter alia, "using a stega-cipher to steganographically encode independent information including a digital watermark into the carrier signal...." Independent Claim 29 contains similar language. The 102 rejection based on Bender is improper for at least the reason that Bender fails to disclose the use of a stega-cipher as required by the rejected claims.

Simply put, the "key" allegedly disclosed in Bender is not the same as a stega-cipher used to steganographically encode independent data into a carrier signal within the meaning of the present claims. In fact, there are several differences between a stega-cipher as used in the

present invention, and the alleged "key" described in Section 3.4 of Bender. As stated in Bender:

> In [Direct Sequence or "DS"], a "key" is needed to encode the information and the same "key" is needed to decode it. The key is pseudo-random noise that ideally has flat frequency response over the frequency range, i.e., white noise. The key is applied to the coded information to modulate the sequence into a spread spectrum sequence.

(Bender at 171). With Bender, the same "key" is used for both encoding and decoding. The stega-cipher being used in the present invention is not so limited. With the present invention, the encode and decode keys may be symmetric or asymmetric depending on the application. Bender's "key" is not ciphered in any manner, but is simply a pseudo-random sequences based on the white noise inherent to the signal. Moreover, even for symmetric applications of the present invention where the encode key and decode key may be the same, the actual mapped locations may be different for each copy encoded of a given carrier signal.

Spread spectrum "is designed to encrypt a stream of information by spreading the encrypted data across as much of the frequency spectrum as possible." (Bender at 171). Spread spectrum spreads the encrypted data across the spectrum by using a "key" that has "maximum randomness and flat frequency spectrum." (Bender at 172). Bender's "chip" or "key" "is a pseudo-random sequence modulated at a known rate." (Bender at 171). This is very different than the stega-cipher of the present invention.

As disclosed in the specification the "stega-cipher" borrows from both steganography and encryption:

> The invention draws on techniques from two fields, cryptography, the art of scrambling messages so that only the intended recipient may read them, and steganography, a term applied to various techniques for obscuring messages so that only the intended parties to a message even know that a message has been sent, thus it is termed herein as a stega-cipher. The stega-cipher is so named because it uses the steganographic technique of hiding a message in multimedia content, in combination with multiple keys, a concept originating in cryptography. However, instead of using the keys to encrypt the content, the stega-cipher uses these keys to locate the hidden message within the content. The message itself is

encrypted which serves to further protect the message, verify the validity of the message, and redistribute the information in a random manner so that anyone attempting to locate the message without the keys cannot rely on pre-supposed knowledge of the message contents as a help in locating it.

(Patent Application at p. 7, lines 13-25). Basically, the steganographic portion of the stega-cipher seeks to identify locations within the carrier signal where information may be stored, but it is the cipher portion of the stega-cipher determines which of those identified locations will be actually used. If all of the locations are used, then it will be easier for others to remove the encoded information, because you can run similar algorithms to identify the candidate locations. The cipher portion uses a mask to encode the independent data into those identified areas, such that not all of the available locations are used. Hence, a hacker will have to wipe out all or almost all of the identified areas to remove the watermark (or simply guess at the potential locations), which generally will degrade the quality of the carrier signal significantly. Bender's key has no such masking. Accordingly, a "stega-cipher" is not the same as Bender's "key."

Moreover, there are differences in how the present invention and how Bender's system detect and read the respective encoded information. Bender's system requires that the "key stream for encoding is known by the receiver" and, in addition, the "following parameters are known by the receiver: chip rate, data rate, carrier frequency, and the data interval." (Bender at 172). This is a lot of information that must be known to decode the encoded data. In the present invention, one only needs a stega-cipher to decode.

A stega-cipher, unlike spread spectrum, seeks to maximize the imperceptibility by limiting the number of bits being encoded. This is antithetical to spread spectrum's adding white noise because to encode data as flat spectrum noise requires significantly more data to be encoded. This point is evidenced by the differences between the seeding of Bender's "chip" and the seeding of a stega-cipher of the present invention. Bender's "chip" is a pseudo-random sequence modulated at a known rate." (Bender at 171). Each bit in Bender's chip is encoded into the signal, whereas with a stega-cipher, only select bits are encoded. Moreover, with a stega-cipher, it is possible that each encoding yields a completely different result as to where watermarks are located. This is a very different result from that contemplated by Bender.

Because Bender fails to disclose a "stega-cipher" as required by claims 25 and 29, the 102 rejection of 25 and 29 must be withdrawn. Moreover, for the same reasons that claims 25 and 29 are patentable over Bender, the claims that depend from claims 25 and 29 are also patentable. Applicant requests the Examiner to withdraw all 102 rejections.

b)   Rejections of certain dependent claims

The Examiner asserts that claims 33 and 35are anticipated by Bender, yet he fails to articulate any basis for these assertions. Claims 33 and 35 include the further step of creating a derivative of the encoded signals. None of the arguments articulated by the Examiner appear directed to claims 33 or 35. For this reason, Examiner has failed to establish a prima facie case of anticipation. Moreover, because Bender fails to teach or suggest "generating a first derivative encoded signal" as disclosed in Claim 33 or claim 35, the rejections based on 102 are improper. For this additional reason, Applicant requests that the 102 rejections of claims 33 and 35 be withdrawn.

III.   103 REJECTIONS

The Examiner asserts that <u>dependent</u> claims 26, 30, 34, 36--61, are obvious in view of Bender, either by itself or in combination with various other references. (Office Action, pp. 2-8).

In order to establish a prima facie case of obviousness, three elements must be established: 1) there must be some motivation or suggestion to make the proposed combination or modification of the references; 2) There must be a reasonable expectation of success; and 3) The prior art reference (or references when combined) must teach <u>all</u> of the limitations of the claimed invention. <u>See generally</u> MPEP 2143. "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must be found in the prior art, not in applicant's disclosure." MPEP 2144 (citing <u>In re Vaeck</u>, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

1. The Combination Of References Fail To Disclose All Of The Claimed Limitations.

a) Complete Failure to Address the "Stega-cipher" Limitation

Setting aside for a moment the first two elements, it is clear that the Examiner has failed to meet the third criterion because the cited references, either alone or in combination, failed to disclose all of the claimed elements. All of the Examiner's rejections are based in whole or in part upon Bender. The previous amendment added the term "stega-cipher" to both independent claims in the application (Claims 25 & 29), and since the Examiner has taken the position that reliance upon Bender is necessitated by the amendment, it is reasonable to deduce that the Examiner relies exclusively on Bender for the teaching of a "stega-cipher." (If the other references taught the use of a stega-cipher, there would have been no need to rely on Bender). This deduction seems to be confirmed by the Examiner's repeated citation that Bender teaches "encrypting digital watermarks into information with a key."

As discussed above, Bender fails to disclose the use of a stega-cipher as required by Claim 25 or claim 29 (or as required by any of the dependent claims). For at least this reason, the Examiner has failed to establish a prima facie case of obviousness for the claims that depend from Claims 25 and 29. Thus, the 103 rejections of 26, 30, 34, 36-61cannot stand.

Noticeably absent from the Examiner's 103 rejections is any discussion whatsoever of the claimed invention's use of a stega-cipher. A careful comparison of the rejections in the Office Action dated March 27, 2001 ("Current OA"), with the rejections in the Office Action dated February 25, 2000 ("Prior OA"), only underscores that the Examiner has not given any patentable weight to the use of "stega-cipher." The rejections in these two office actions are substantially verbatim, with the sole exception that the Examiner has substituted "Bender" for "Schneier" and/or other references. Compare Current OA ¶ 6 with Prior OA ¶11; Current OA ¶ 7 with Prior OA ¶13; Current OA ¶ 8 with Prior OA ¶14; Current OA ¶ 9 with Prior OA ¶15; Current OA ¶ 10 with Prior OA ¶8; Current OA ¶ 11 with Prior OA ¶10; Current OA ¶ 12 with Prior OA ¶16; Current OA ¶ 13 with Prior OA ¶17; and Current OA ¶ 13 with Prior OA ¶19. It would seem logical that if the amended claim language had received any consideration, it would

have appeared in at least one of the 103 rejections. Nevertheless, Applicant will step through these cut-and-pasted rejections in order to demonstrate careful consideration of each of the rejections.

b)   Misreading of Bender

In the Office Action, the Examiner pointed out that Bender distinguishes steganography from encryption. (Office Action at 2). The key distinction lies in whether the perceptible characteristics of the underlying data are changed. Steganography seeks to hide a message into the underlying data without changing its perceptible characteristics (i.e., "hide the message in plain view"). Encryption seeks to change the underlying data so that it is no longer recognizable.

Examiner's comments regarding Bender and certain other references suggest that the Examiner has misinterpreted the references. For example, Examiner states several times that "Bender et al. teaches encrypting digital watermarks into information with a key." (See ¶¶ 6, 7, 8, 9, 10 and 11 of the Office Action). This assertion is inaccurate.. It may be fair to characterize Bender to teach encoding watermarks into information, but Bender does not teach "encrypting watermarks into information." Applicant has construed Examiner's assertion to mean that Bender teaches encoding watermarks into information. If this assumption is inaccurate, please advise. This point is raised because it is not clear whether the 103 references have been properly construed in light of the distinction between steganography and encryption.

c)   Bender in view of Barton

Examiner rejects claims 26, 30, and 52-54 as unpatentable over Bender in view of Barton. In addition to the reasons stated above, Applicant submits that this rejection is improper because the combination of Bender and Barton does not yield the claimed invention unless the Examiner uses impermissible hindsight based on Applicant's invention to make the combination.

Claim 52 relates to "adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream." Implicit in Claim 52 is that multiple watermarks exist in the same sample stream. The Examiner has not established where

Bender (or even Barton) teaches the use of multiple watermarks. Unless you have multiple watermarks, there is no need to consider marking them with unique data.

Further, the Examiner has read Barton using impermissible hindsight. Barton provides:

> The invention provides a method and apparatus for basic authentication of a digital block and for carrying additional authentication information provided by the user, i.e. meta-data, in a secure and reliable fashion. To embed authentication data into a digital block, a digital signature is formed that is a reduced representation of the digital block. The signature and additional information supplied by the user are embedded into the digital block by replacing predetermined bits within the block. Encryption can be used to enhance authentication capability. The encrypted data can be further verified using error correction coding techniques. For sequential data, such as the frames of a video display, a sequence numbers can also be provided as part of the meta-data to ensure that frames have not been deleted or re-ordered.

(U.S. Patent No. 5,912,972, Col. 4, lines 18-33). As understood, Barton encodes authentication information into a digital block by first making a digital signature of the digital block, adding meta-data provided by the user, and then encoding the digital signature and the meta data into the digital block. Barton further suggest that where the underlying data comprises sequential data such as video frames (for example, where the digital blocks represent video frames), the meta data being added can include frame numbers to indicate the sequence order. It would appear that the Examiner's argument has assumed that the meta-data represents a watermark (because it represents independent data provided by the user). Thus, at best Barton suggests that unique information about the underlying data can be added to the meta data to provide information about the underlying data. Claim 52 is directed to the unique identification of multiple watermarks that may be imbedded into underlying data. Barton appears to teach the unique identification of the underlying data. The motivation for marking Barton's underlying data is based upon the purpose of the underlying data (e.g., video frames). This motivation does not suggest any need or desire to uniquely mark the data that is being embedded into the underlying data. So, even if you assume a motivation for combining Barton and Bender, you still do not have the invention of Claim 52, and therefore claim 52, and claims 53 and 54 that depend from claim 52, are not obvious. The rejection must be withdrawn.

d)   Bender in view of Braudaway

Examiner rejects claims 38 and 39 as unpatentable over Bender in view of Braudaway. In addition to the reasons stated above, Applicant submits that this rejection is improper because the combination of Bender and Braudaway does not yield the claimed invention unless the Examiner uses impermissible hindsight based on Applicant's invention to make the combination.

The Examiner has failed to establish a prima facie case of obviousness to support the rejection of claims 38 and 39. The examiner asserts that in "the abstract, Braudaway et al. say that certain pixels brightness are altered as a result of the watermark." From this mere assertion, the Examiner concludes that "This change in brightness anticipates claims 38's spectral values." (Office action at 6). This conclusion is completely unsupported by any reasoning. The Examiner has not identified any portion of Braudaway that discloses "decoding a single message bit from a single spectral value," and for this additional reason, the rejection is untenable.

The examiner further asserts that "in the abstract, Braudaway et al. talk about using only certain non-transparent values of the watermark." From this assertion, the Examiner concludes, "These non-transparent values form a map to meet claim 39." This conclusion too is completely unsupported by any reasoning. Braudaway, in fact, does not reference any "map." The Examiner's logic has not been expressed, and therefore, it would appear sufficient to say that Braudaway does not disclose the step of "using a map table to define where watermark information is to be encoded based on random or pseudo-random masks into the carrier signal, wherein the map table is defined such tat any index of the map table enables encoding information" as required by the rejected claim. For this additional reason, the rejection must be withdrawn.

e)   Bender in view of Schneier

Examiner rejects claims 40-43 and 46-48 as unpatentable over Bender in view of Schneier. Examiner also rejects claims 50-51 as unpatentable over Bender in view of Schneier and Barton, and claims 44, 45 and 49 as unpatentable over Bender in view of Schneier and Cox.

In addition to the reasons stated above, Applicant submits that this rejection is improper because the combination of Bender and Schneier does not yield the claimed invention.

The Examiner relies on Schneier's discussion of the Digital Encryption Standard as follows:

> Chapter 10 of Schneier deals with the Digital Encryption Standard. DES uses an effectively 56-bit key. As described on pages 224-226, this key is broken down and permuted into the encryption of block data. The key breakdown and the subsequent permutation correspond to applicant's [sic, Applicants'] mask set. DES uses starting vectors and padding at the end of messages. These correspond to the start of message delimiter and number of bytes to follow the message of [Applicants'] claims 42 and 47. Claims 43 and 48 are anticipated by DES' mixing of the two 32-bit blocks and the integration of the key. It would have been obvious . . . to encrypt the key-encrypted watermark data of Schneier with DES because DES is an encryption standard.

(Office Action, pp. 6-7). DES is an encryption standard, but DES is not the same as steganographic ciphering. DES processes data without regard to the perceptibility of the data. Thus, there is no "mask set" in a DES cipher. Contrary to the Examiner's assertion, the key breakdown and permutations are simply data, and bear little relationship, if any, to the mask set claimed in the present application. Further, Applicants note that the Examiner has not provided any support for the assertion that the key breakdown and permutations "correspond to the start message delimiter and number of bytes to follow the message of [Applicants'] invention." Id.

The rejected claims rely on the use of a "mask set." Because Schneier fails to disclose or suggest the use of a mask set as disclosed in the claims (whether alone or in combination with the other references), and even fails to disclose the use of a stega-cipher, the rejections of claims 40-48, and 49-51 must be withdrawn.

f)   Rejection of Claim 34

The Examiner asserts that Claim 34 is obvious in view of Bender, yet the basis provided for this assertion does not appear to be related to Claim 34. Examiner asserts that "it would have been obvious to a person of ordinary skill in the art at the time the invention was made to protect

the watermarked data of Bender et al. by encrypting it." (Office Action at 4). Claim 34 is directed, in part, to "modifying the first derivative encoded signal" that was initially referenced in Claim 33. The arguments articulated by the Examiner do not appear to be directed to claim 34. For this reason, Examiner has failed to establish a prima facie case of obviousness. Moreover, because Bender fails to teach or suggest "generating a first derivative encoded signal" as referenced in Claim 33 and 34, the rejection based on 103 is improper. For this additional reason, Applicant requests that the 103 rejection of claim 34 be withdrawn.

2.   The is no motivation to combine Bender with the other references.

a)   Generally

The examiner has failed to establish a prima facie case of obviousness to the extent that there is no motivation or suggestion to make the proposed combinations of the references as directed by the Examiner. More particularly, there is no motivation to combine Bender with the following references: Morris; Powell; Braudaway; Schneier; and Cox

According to the MPEP,

[i]n order to support a conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention obvious in light of the teachings of the references.

MPEP 2142 (citing Ex parte Clapp, 277 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985) (emphasis added). Further, "[w]hen the motivation to combine the teachings of the references is not immediately apparent, it is the duty of the examiner to explain why the combination of teachings is proper." MPEP 2142 (citing Ex Parte Skinner, 2 USPQ2d 1788 (Bd. Pat. App. & Inter. 1998)).

The Federal Circuit has recently emphasized the importance of providing evidence of motion to combine in Winner int'l Royalty Corp. v. Ching-Rong Wang, No. 98-1553 slip op. at 14 (Fed. Cir. Jan. 27, 2000). "Although a reference need not expressly teach that the disclosure contain therein should be combined with another . . . the showing of combinability, in whatever

form, must nevertheless be 'clear and particular.'" Winner at 15 (citations omitted). Further, the "absence of such a suggestion to combine is dispositive in an obviousness determination." Gambro Lundia AB v. Baxter Healthcare Corp., 11 F.3d 1573, 1579 (Fed. Cir. 1997)..

Applicant submits that the Examiner has not satisfied his initial burden of providing "clear and particular" evidence of motivation to combine. Instead, it appears that the Examiner has simply identified references that allegedly disclose the elements of the claim, and has combined them. Even assuming arguendo that the references contained all elements of the claimed invention, it is still impermissible to reject a claim as being obvious simply "by locating references which describe various aspects of a patent applicant's invention without also providing evidence of the motivating force which would impel one skilled in the art to do what the patent applicant has done." Ex parte Levengood, 28 USPQ2d 1300, 1303 (Bd. Pat. App. & Inter. 1993) (emphasis added).

b)   Detailed discussion of Morris

There is no motivation to combine Bender with Morris. The Examiner relies on Morris to suggest that "a one bit change of the least significant bit ... can be used to carry identification codes" and, therefore, it would have been obvious "to discreetly carry the watermark information of Bender et al. in the least significant bits as taught by Morris." (Office Action at 4). Bender and Morris appear to be incompatible. Bender uses spread spectrum techniques to spread data out over a frequency range. The output is a composite analog signal—not digital. There is no opportunity to insert information into the LSB of Bender's carrier signal as suggested by the Examiner. In fact, Bender teaches away from such an LSB technique because it is too easy to break. (See generally Section 3.2 of Bender, p. 170). Equally important, it is not readily apparent that there is a reasonable likelihood of success in combining these two techniques. Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claim 34 based on the combination of Bender and Morris must be withdrawn.

c)   Detailed discussion of Powell

There is also no motivation to combine Bender with Powell. Powell is directed to images, while Bender's spread spectrum is directed to audio. As the Examiner asserts, Powell teaches "a method of embedding [that] requires use of a map of an image to determine the places to embed the watermark." (Office Action at 5). Because Powell's technique is directed specifically to the use of an image, and Bender is directed specifically to spread spectrum techniques for audio, it is not readily apparent why one would want to combine these references. Equally important, it is not readily apparent that there is a reasonable likelihood of success in combining these two techniques. Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claim 37 based on the combination of Bender and Powell must be withdrawn.

d)   Detailed discussion of Braudaway

Similarly, there is also no motivation to combine Bender with Braudaway. Braudaway is directed to images, while Bender's spread spectrum is directed to audio. As the Examiner asserts, Braudaway teaches "a method of embedding [that] requires use of a map of an image to determine the places to embed the watermark." (Office Action at 5). Because Braudaway's technique is directed specifically to "Color Correct Digital Watermarking of Images" (see title of U.S. Patent No. 5,530,759), and Bender is directed specifically to spread spectrum techniques for audio, it is not readily apparent why one would want to combine these references. Equally important, it is not readily apparent that there is a reasonable likelihood of success in combining these two techniques. Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claims 38 and 39 based on the combination of Bender and Braudaway must be withdrawn.

e)   Detailed discussion of Schneier

There is also no motivation to combine Bender with Schneier. The Examiner relies on Schneier's discussion of DES. As explained above, DES is an encryption standard. Bender purports to relate to data hiding (i.e., steganography). (See the Title and Abstract to Bender).

Absent the hindsight gained by Applicant's invention, there is no motivation to combine the DES of Schneier with the data hiding techniques of Bender. Equally important, it is not readily apparent that there is a reasonable likelihood of success in combining these two techniques. Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claims 40-43 and 46-48 based on the combination of Bender and Schneier must be withdrawn.

f)   Detailed discussion of Cox

There is also no motivation to combine Bender, Schneier and Cox. In addition to the preceding section that outlines the differences in Bender and Schneier, the further combination of Cox is equally unsupported. The Examiner's apparent sole evidence of motivation is an assertion that "it would have been obvious . . . to reap the benefits" of Cox. This statement is not "clear and particular" evidence of motivation to combine, as required by the MPEP. What benefits are lacking in Schneier that are provided by Cox? Moreover, it would appear that Schneier and Cox are teaching incompatible techniques, and so, why would one skilled in the art combine them? In the absence of motivation to make the proposed combination of references, Applicants respectfully request that the rejection of claims 44, 45, and 49 be withdrawn.

REQUEST FOR RECONSIDERATION

Applicant respectfully requests that the Examiner reconsider the application in view of the foregoing remarks, to withdraw the finality of the last office action, and to withdraw the rejections of all pending claims.

CONCLUSION

Applicant respectfully submits that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that an interview with Applicant's representative, either by telephone or in person, would further prosecution of this application, we would welcome the opportunity for such an interview.

Respectfully submitted,

WILEY REIN & FIELDING LLP

Date: October 25, 2001   By:_____

Wiley Rein & Fielding LLP   Floyd B. Chapman
1776 K Street, N.W.   Registration No. 40,555
Washington, D.C. 20006
202.719.7000 (Telephone)
202.719.7049 (Facsimile)